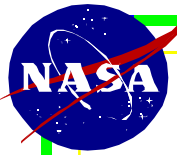


Network Security: From Firewalls to Internet Critters—Some Issues for Discussion

Slide 1

ADNET

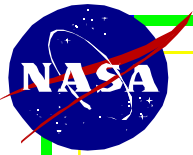


Presentation Contents

- Firewalls
- Viruses
- Worms and Trojan Horses
- Securing Information Servers

Slide 2

ADNET

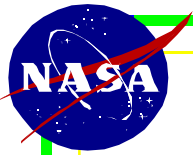


Section 1:

Firewalls—What they are and how to build them

Slide 3

ADNET

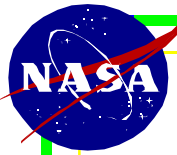


What is a Firewall?

- A barrier between internal and external environments, designed to prevent outsiders from accessing your data.
- Offer the greatest security by giving multiple levels of protection while allowing necessary services.
- Not necessarily a single piece of hardware or software.
- Audit or log Internet usage, keep statistics
- Act as a central point of contact

Slide 4

ADNET

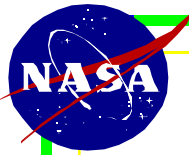


Firewalls

- What are the threats
 - Curious crackers
 - Vandals
 - System Downtime
 - Network Outages
 - Telephone line use
 - Accidental data disclosure
 - Privacy issues

Slide 5

ADNET

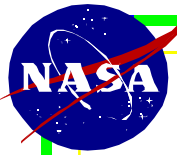


Firewalls

- Network Security Paradigms
- That which is not expressly permitted is prohibited
 - **firewall blocks everything** □ **services must be individually enabled on a case by case basis**
 - **Administrator must take steps to support each service**
 - **Users may see firewall as a hindrance**
- That which is not expressly prohibited is permitted
 - **Firewall blocks services that are known security risks**
 - **Users can potentially introduce security holes in system**

Slide 6

ADNET

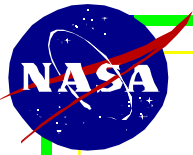


Some Questions to Ask

- If the firewall is breached, what kind of damage could be done to private net?
- How big is the zone of risk?
- How easy is it to detect that a break in or destruction has occurred?
- How much audit information will be kept for diagnosis?
- How inconvenient is the firewall to the users?

Slide 7

ADNET



Firewall Precautions

- Do not run Network Information System (NIS) on the firewall (like having the Yellow Pages)
- Ensure strong passwords and filesystem protection on the firewall
- Eliminate all non-essential services
- Do not mount remote NFS filesystems on the firewall machine
- Enable extensive logging
- Don't allow user accounts on firewall machines

Slide 8

ADNET



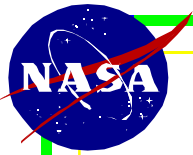
Firewall Costs

- Obvious Costs
 - Hardware
 - Software
- Hidden Costs
 - Maintenance
 - Administration
 - Loss of Services Due to Security
 - Violation Potential
 - Training



Slide 9

ADNET



Firewall Categories

Screening Routers

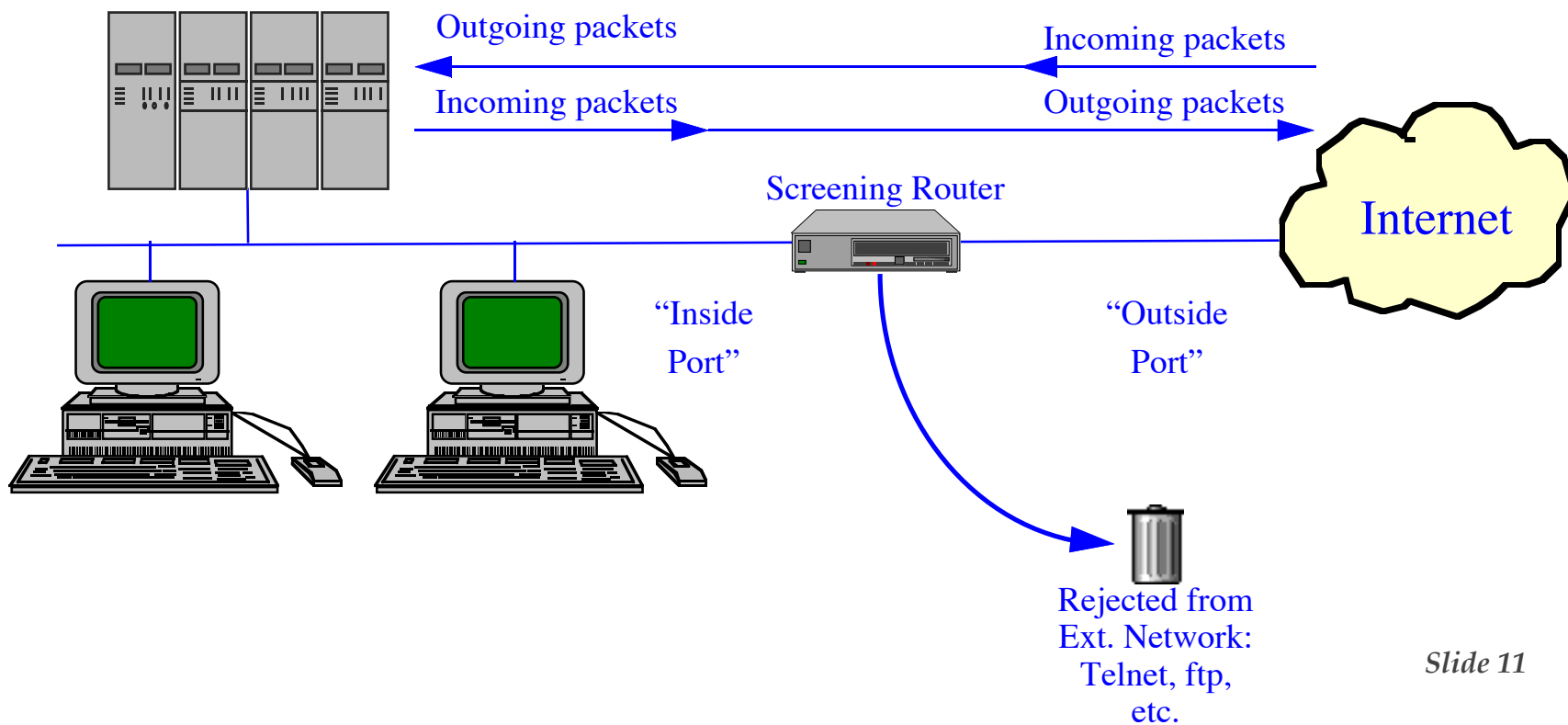
- Least secure method
- Can be a commercial router or host that supports packet screening, eg Cisco, Proteon, 3Com
- Block traffic between networks, hosts, IP ports, protocols or packet types
- Some screening routers permit various levels and types of packet logging
- May be the only component in a firewall
- Design Philosophy - "That which is not expressly prohibited is permitted"

Slide 10

ADNET

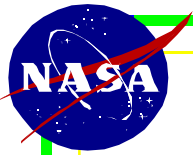


Screening Router Placement



Slide 11

ADNET

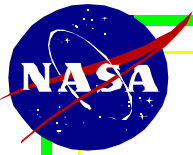


Packet Filter Questions

- ◆ Where is the filtering to be done? On input, output, or both?
- ◆ What attributes (i.e. protocol, source, destination, etc) can be checked?
- ◆ How are protocols other than TCP, UDP handled?
- ◆ Can source routed packets be rejected?
- ◆ How comprehensible is the filter language? Can you control the order of application of the rules?

Slide 12

ADNET



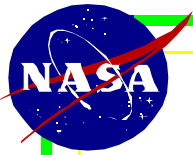
Firewall Categories

Risks of Screening Routers

- Very minimal logging information
- Difficult to configure screening rules
- Entire network can be unprotected if firewall is breached
- Addition of new services may open holes
- Can be bypassed by tunnelling, eg DNS.
- Can be vulnerable to source routed traffic
- Some protocols not suited to packet filtering, eg rcp, rlogin, rsh, rdist, NFS, NIS

Slide 13

ADNET



Firewall Categories

Bastion Hosts

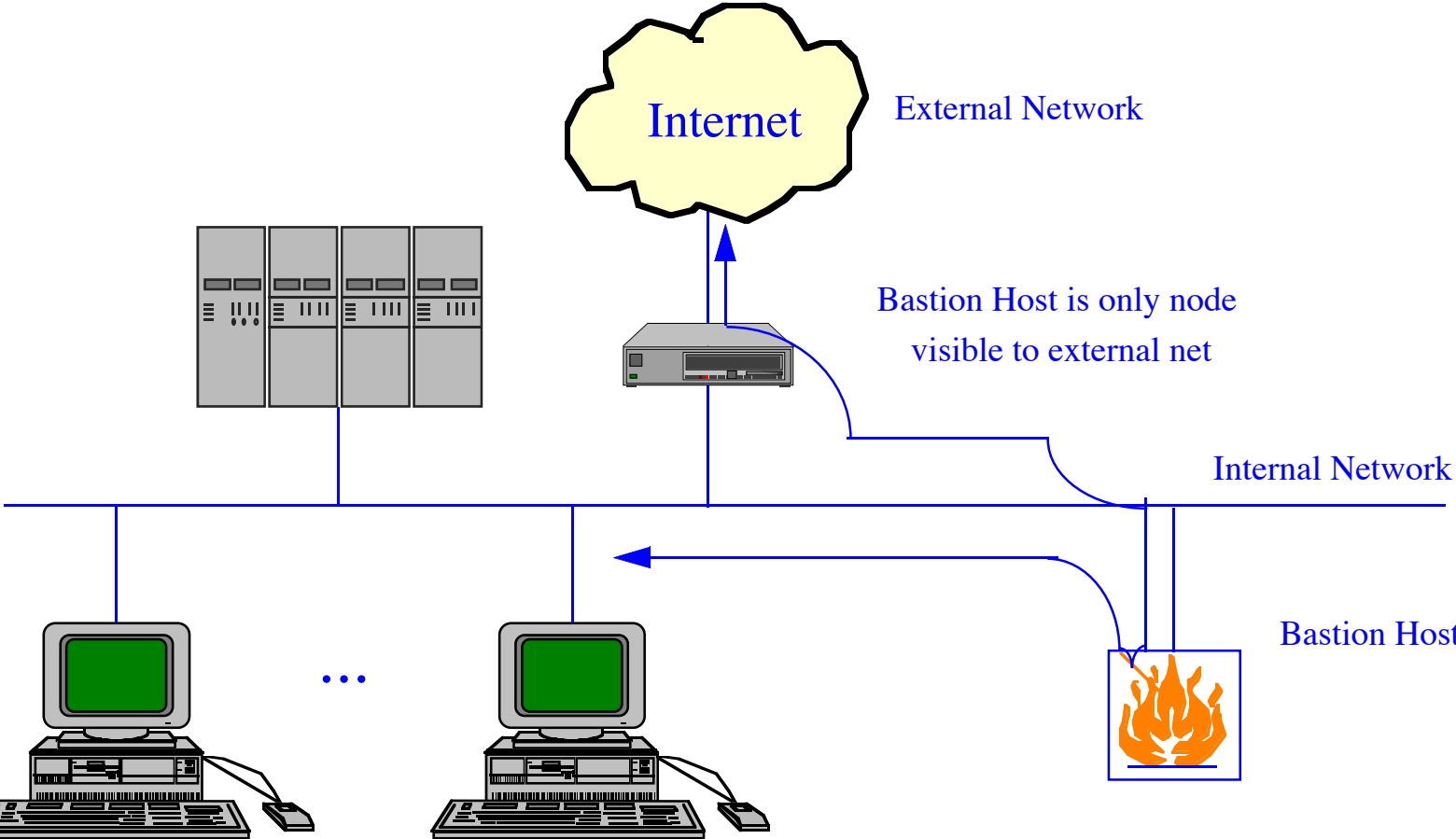
- Only system visible to external network
- Special systems identified as network “strong points”
- Often act in capacity of E-mail relays, name servers, FTP servers, Usenet servers etc.,.
- Generally, a Bastion Host is one that is recognized as a potential point of attack and will have extra attention paid to its security, audits, software etc.
- Should not be “trusted”

Slide 14

ADNET

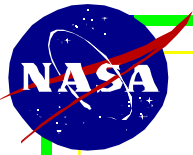


Bastion Host



Slide 15

ADNET



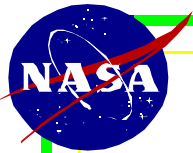
Firewall Categories

Dual Homed Gateway

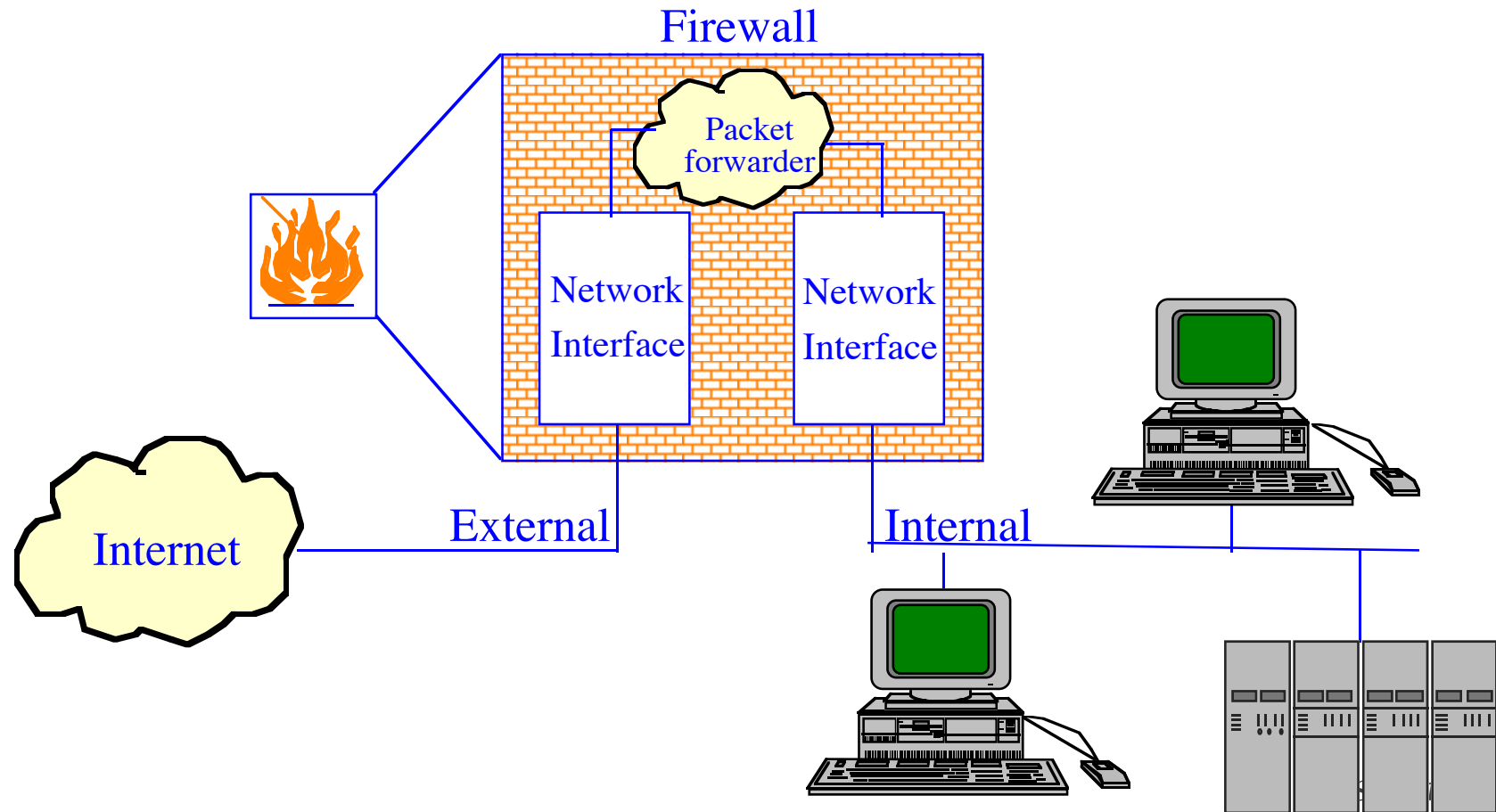
- Special case of Bastion Host
- Reachable from both Internet and private network, with IP forwarding turned off (direct traffic between the networks is blocked)
- All traffic relayed through application level filters, must pass security checks before being passed on
- No user login accounts allowed on the system
- All connections are logged so that a complete audit trail is available

Slide 16

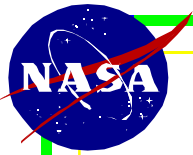
ADNET



Dual Homed Gateway



ADNET



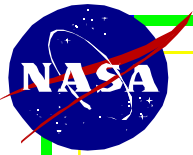
Dual Homed Gateway

Disadvantages:

- difficult to set up properly
 - turning off IP source routing
- difficult to manage
 - large number of users
 - usually require a number of services
- inconvenient to use
 - users first have to access the dual homed host and then access services (services can't be accessed directly from the desktop)

Slide 18

ADNET



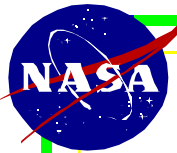
Firewall Categories

Screened Host Gateway

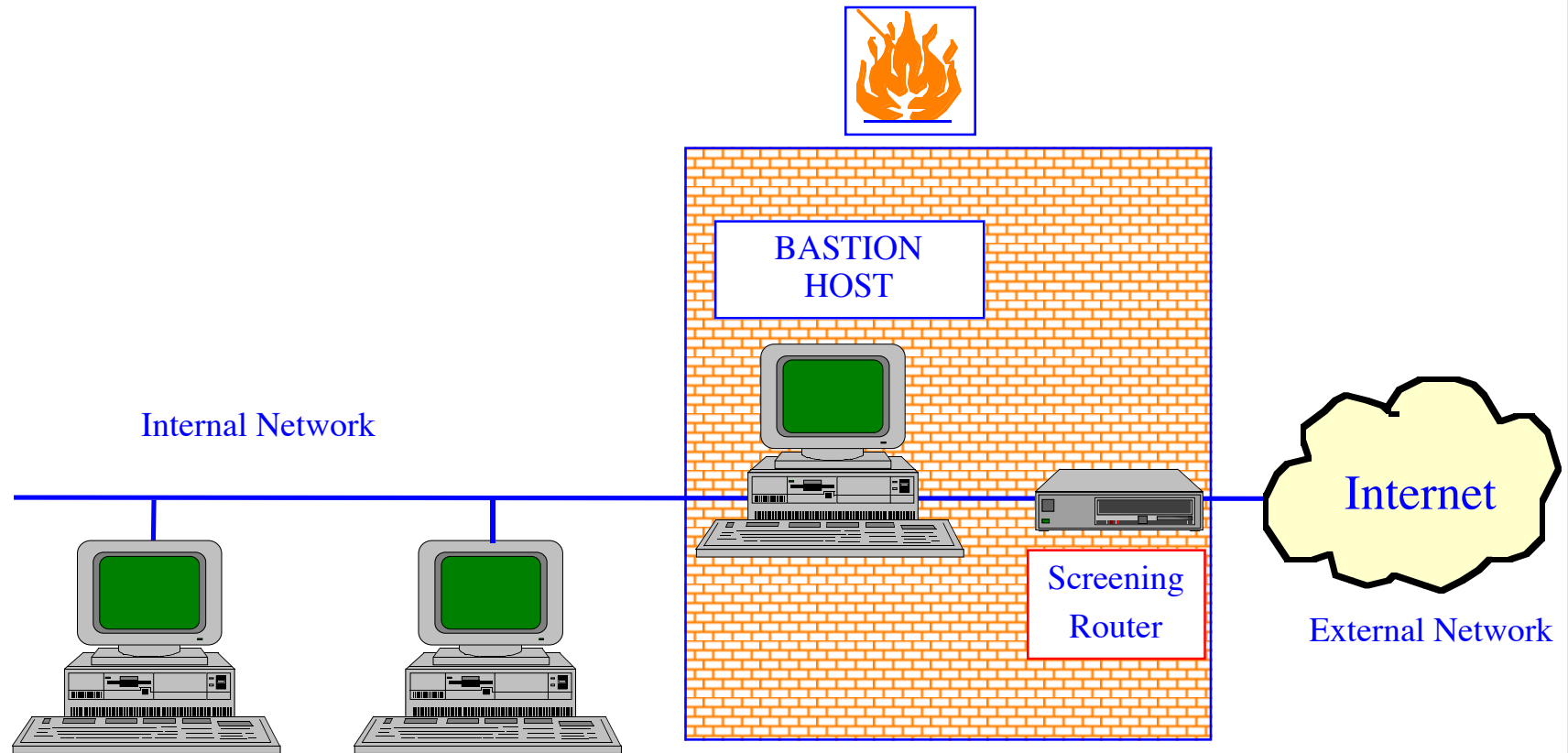
- Most common and flexible form of Firewall
- Screening Router blocks traffic between Internet and all hosts on private network except for a single Bastion Host
- Screening Router can be configured to permit nodes on private network to directly access Internet via Telnet or FTP.
- Screening router is usually configured to block traffic to the Bastion host on specific ports

Slide 19

ADNET

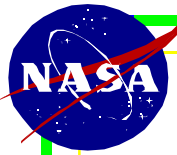


Screened Host Gateway



Slide 20

ADNET



Screened Host Gateway

■ Advantages:

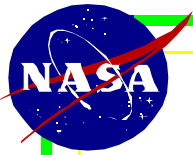
- added security over a single bastion host
- fairly easy to implement

■ Disadvantages:

- requires a router and a bastion host
- intruder detection depends on logging procedures

Slide 21

ADNET



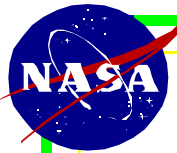
Firewall Categories

Screened Subnet

- Creates isolated subnet between Internet and private network
- Internet can only communicate with nodes on the Screened Subnet
- Private network nodes can only communicate with nodes on the Screened Subnet
- The private network becomes effectively invisible to the Internet

Slide 22

ADNET



Screened Subnet

■ Advantages:

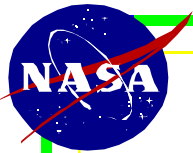
- sandbox or demilitarized zone between the protected network and the Internet
- direct traffic across the screened subnet is blocked
- Only the Bastion host is at risk
- good for high volume and high speed traffic

■ Disadvantages:

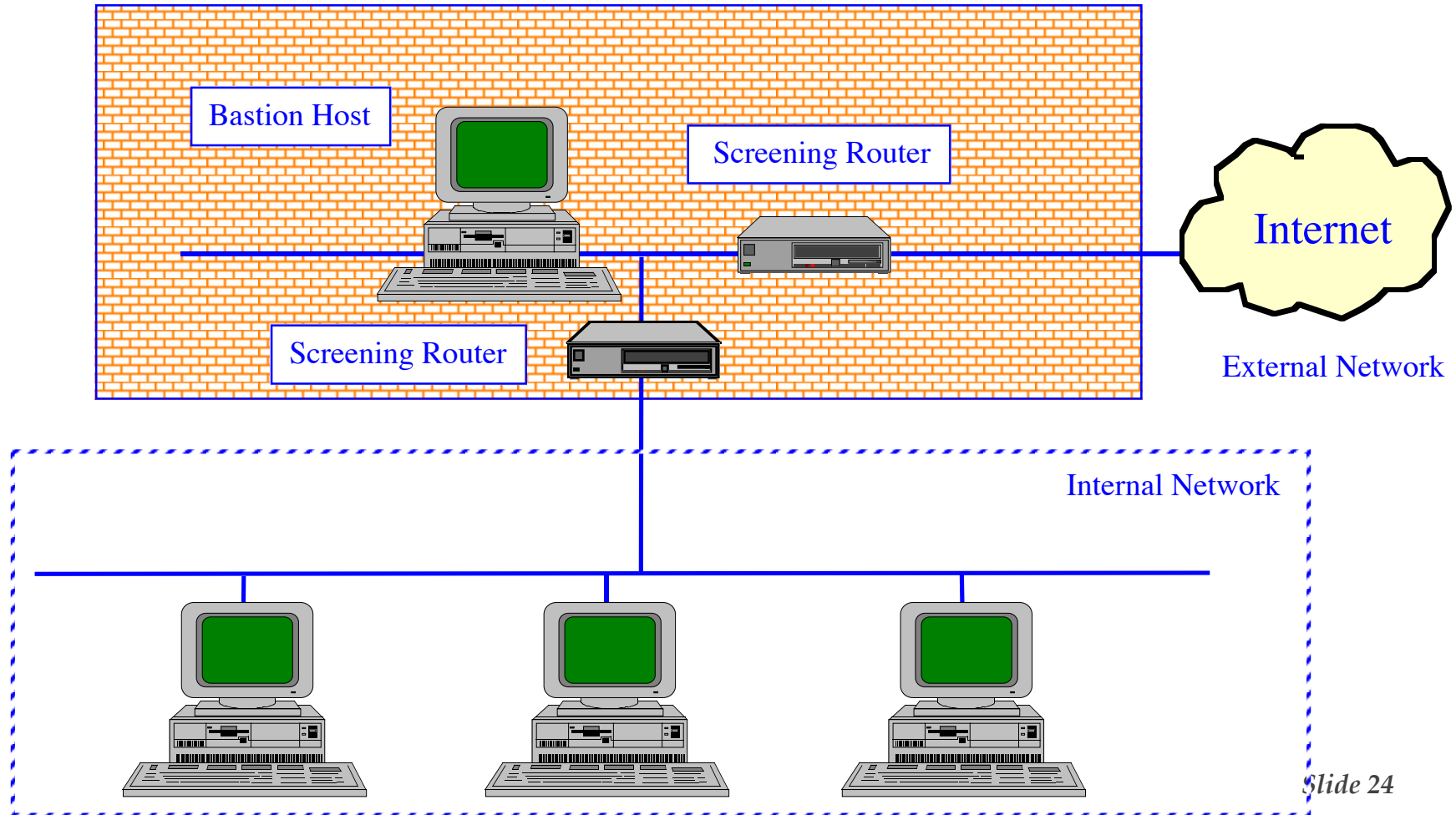
- complexity of configuring screening routers
- entire network is reachable from the outside if screening routers fail

Slide 23

ADNET

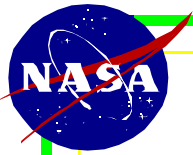


Screened Subnet



Slide 24

ADNET



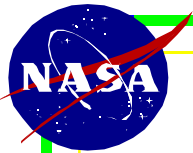
Firewall Categories

Proxy or Application Gateway

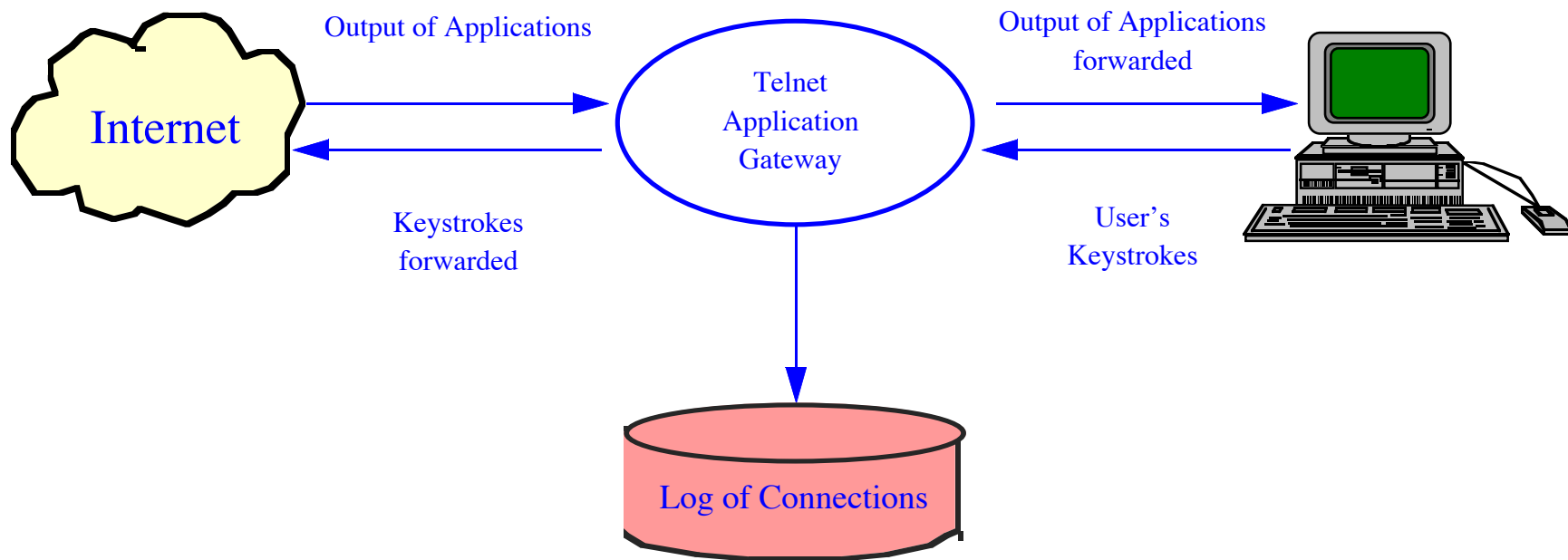
- Handle store and forward traffic and some types of interactive traffic
- Handle traffic at an application level
- Can easily log/audit traffic
- Can have extra security built in as needed
- Examples:
 - **Sendmail**
 - **Telnet**
 - **FTP**
 - **Web Server**

Slide 25

ADNET

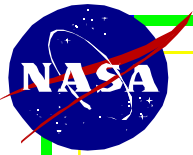


Telnet Application Gateway



Slide 26

ADNET

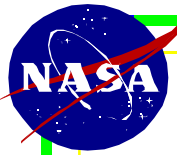


Evaluating Application Gateways

- What applications are supported? (mail, gopher, X11)
- Are specialized client programs needed?
- How are the difficult services, such as FTP and X11, handled?
- Are the logging, access control, and filtering routines adequately documented?
- What sorts of logs and authentication mechanisms are provided?
- Are any traps or lures provided? Can you add your own?

Slide 27

ADNET



Application Gateways

■ Advantages:

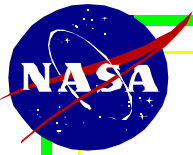
- allow users to access internet services directly
- good logging procedures
- provide some form of authentication

■ Disadvantages:

- new services need to be provided
- burden the firewall administrator
- proxy services are not workable for some services
- require two steps to connect inbound and outbound traffic

Slide 28

ADNET



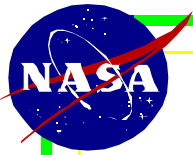
Firewall Summary

- Use Common Sense
- Keep It Simple
- Trial and Error
- Use Help Resources
- Rely on the tools you know and understand



Slide 29

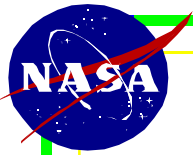
ADNET



Section 2: Viruses and how to combat them

Slide 30

ADNET

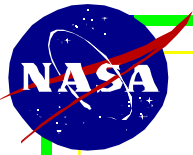


Viruses

- “Infect” computer executable programs by attaching themselves to these programs
- May contain a “trigger” to perform some specific act when certain conditions are met
- Once infected, a program will infect other programs when it executes, thus spreading the virus
- Can be downloaded with programs off the Internet
- Most are benign, but may cause erratic behavior□
- Cannot infect a computer via e-mail, or infect data
- Various virus tools are available to counteract them

Slide 31

ADNET

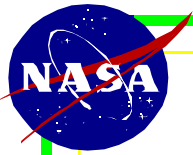


Virus Examples

- The WDEF Virus causes computer to beep, frequently crash or display fonts incorrectly
- nVIR Virus causes computer to beep every 8 to 16 times it is started
- A newly discovered Mac Virus called "HC 9507" infects the HyperCard application.
- HC 9507 does not infect system files or other applications
- May cause screen to fade in and out, type "pickle" automatically or a system shutdown or lockup.

Slide 32

ADNET

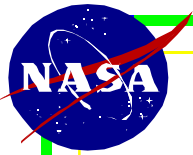


Virus Tools

- Detect the presence of a virus on a system
- Static Analysis—can inspect diskettes before installation, or test system on a regular basis
- Interception—halt the execution of an infected program as the virus attempts to replicate
- Modification—search for the unexpected modification of programs
- Identification—identify which particular virus has infected a system
- Removal—attempt to remove all viruses

Slide 33

ADNET

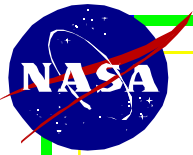


Virus Tools Selection Factors

- Accuracy
 - Detection Tools—false positives, false negatives
 - Identification—fails to correctly identify virus
 - Removal—hard failure and soft failure
- Ease of use—difficulty in using system, presentation of results
- Administrative Overhead—load on technical support team
- System Overhead—load on system

Slide 34

ADNET

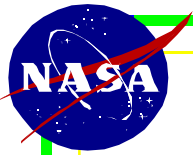


Section 3:

Internet Worms and Trojan Horses—descriptions and some examples

Slide 35

ADNET

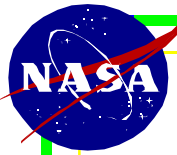


Internet Worms

- Use Network services to propagate
 - Network mail utility
 - Remote execution capability
 - Remote login capability
- Do not require a “host” program to spread
- Originally designed for useful purpose
- Can spread to many systems very quickly

Slide 36

ADNET



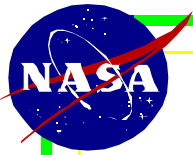
Trojan Horse

Trojan Horse:

- A program that disguises itself by purporting to accomplish some useful function.
- For example, a Trojan horse program could be advertised as a calculator, but it may actually perform some other function when executed, such as modifying files.
- Cannot infect other machines unless it is run on them

Slide 37

ADNET



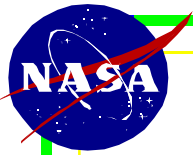
Trojan Horse Example

PKZ300B:

- Version 3.00G of PKWARE's shareware DOS data compression utility
- Distributed as a self extracting archive, PKZ300B.EXE, which contains a Trojan Horse
- If run, will destroy all data on a PC's hard drive
- Will only affect the machine on which it is run
- Latest actual release of PKZip is v2.04G

Slide 38

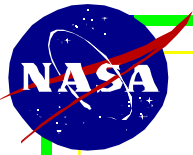
ADNET



Section 4: Securing Internet Information Servers

Slide 39

ADNET

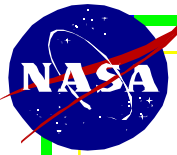


General Guidelines

- Information server should be a dedicated system
- Server process should run with as little privilege as possible
- Server software should be executed in a restricted file space
- Administrators should closely monitor the integrity of the system and information

Slide 40

ADNET

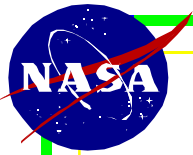


Anonymous FTP Servers

- No files or directories should be owned by user "ftp"
- No encrypted passwords should be in the file '~ftp/etc/password'
- If possible, no files or directories should be writable by anonymous users

Slide 41

ADNET



Web Server Security

- Run the server daemon as a nonprivileged user (“nobody”), rather than as root
- Turn off “Server Includes” or “Server Parsed” options
- Write CGI scripts (for user input) carefully
- Run the server in a restricted portion of the file space (use chroot for Unix)

Slide 42

ADNET